IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

STUDY ON BIOMETRICS AND ITS APPLICATIONS IN INTRUSION DETECTION

Vinayak Marikatti[1], Vaishnavi Mithare[2]

Department of MCA, K.L.S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1]

Department of MCA, K.L.S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[2]

Abstract: The rapid and straightforward association with wireless access points (APs) provides users with quick and temporary access to the Internet. This convenience requires only a few seconds for users to bring their devices to a hotspot and perform minimal configuration to gain Internet connectivity. Biometrics is a technique used in intrusion detection systems to uniquely identify and profile individual users based on various characteristics such as browser settings, behavior patterns, or network activities. This method allows for the detection of unauthorized access and malicious activities within a system. This approach enables the detection of unauthorized access and malicious activities within a system by creating distinct user profiles. By leveraging Biometrics, organizations can not only enhance security against targeted attacks but also personalize services and detect online fraud with greater accuracy. This paper examines the methodologies behind biometrics, its integration into IDS, and the resultant improvements in security measures. We discuss the practical benefits, such as reduced false positives and enhanced detection capabilities, alongside challenges like privacy concerns and computational demands. Our analysis demonstrates that biometrics is a vital tool in modern cybersecurity strategies, offering robust protection against increasingly sophisticated cyber threats.

Keywords: Intrusion detection, Biometrics, keystrokes, Authentication.

I. INTRODUCTION

Biometrics for intrusion detection involve the use of behavioral biometrics to identify and authenticate users. Behavioral biometrics focus on unique behavioral patterns exhibited by individuals, such as keystroke dynamics and mouse movement patterns[5]. Analyzing keystroke dynamics involves studying the rhythm, timing, and pressure applied while typing, which creates a unique typing pattern for each user. By comparing these patterns with a baseline, anomalies can be detected, indicating potential security threats. Similarly, mouse movement patterns can be used for user authentication by analyzing the speed, trajectory, and acceleration of mouse movements, which are unique to each individual [10].The application of user fingerprinting in intrusion detection extends to various domains such as computer networks, controller area networks, and web applications. By employing innovative fingerprinting techniques like temperature-varied ECU fingerprints or deep nearest neighbor website fingerprinting attacks, security professionals can effectively identify and trace intrusion sources, detect fraudulent activities, and protect against various attacks like SQL injection or cross-site scripting.

II. USER FINGERPRINTING

User fingerprinting involves identifying and tracking users based on unique characteristics of their devices or behavior. This technique finds applications in various domains. One key application is in online tracking for advertising, where browser fingerprinting is utilized to collect information about a user's browser configuration and environment.Unlike traditional methods like cookies, browser fingerprinting is challenging for users to control, making it a potent tool for advertisers. User fingerprinting isn't just about behavior or biometrics; it can also tap into device-specific traits[1]. For instance, smartphones have unique features like accelerometers, which measure movement. These accelerometers have distinct patterns that can be used to identify and track users. This means that even if you change settings or browsers, your smartphone's unique "motion fingerprint" can still be used to recognize you.Moreover, motion sensors in smartphones can also be utilized for fingerprinting. These sensors detect movements of the device, which can create a unique pattern for each user. So, by analyzing these motion patterns, websites or apps can track users based on how they move their device. Essentially, it's like your device having its own unique signature based on how it moves, which can be used for identification purposes [1].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

III. BIOMETRICS

Biometrics involves using biological terms and statistical data analysis to confirm a person's identity by examining their physical traits or behaviors. Examples include facial features, fingerprints, voice patterns, signatures, and typing rhythms. Biometric systems gather this data from individuals and use it for comparison each time the person's identity needs to be verified. These systems are composed of three main parts: sensing (capturing data), feature extraction (analyzing and identifying unique characteristics), and matching (comparing the extracted features with stored data)[6],[10].
We can justify the biometric techniques into two ways:

1. Physiological Techniques

Physiological biometric techniques measure inherent physical characteristics that are unique and typically stable over time. Examples include:

1. Facial Analysis: Measures facial features and structures.
2. Fingerprint: Analyzes the unique patterns of ridges and valleys on a person's finger.
3. Hand Geometry: Measures the shape and size of the hand.
4. Retinal Analysis: Examines the unique pattern of blood vessels in the retina.
5. DNA: Analyzes genetic material, which is unique to each individual (except identical twins).

2. Behavioral Techniques

Behavioral biometric techniques measure patterns in a person's behavior, which can be unique but may vary over time. Examples include:

1. Signature: Analyzes the way a person signs their name, including speed, pressure, and style.
2. Keystroke: Measures the rhythm and speed of typing on a keyboard.
3. Voice: Analyzes vocal characteristics like pitch, tone, and speaking style.
4. Smell: Uses the unique chemical composition of an individual's body odor.
5. Sweat Pores Analysis: Examines the pattern of sweat pores on the skin.

Biometric recognition systems utilize unique physical or behavioral traits to either identify or verify individuals. These systems operate in two main ways:

1. Identification Mode: In this mode, the system tries to identify who a person is by searching through a large database of people who have already enrolled. It's like finding a specific face in a crowd of many faces.

2. Authentication Mode: In this mode, the system checks if the person is who they claim to be by comparing their current data (like a fingerprint or face scan) with the data they provided earlier when they enrolled. It's like matching a key to a specific lock to make sure it fits.

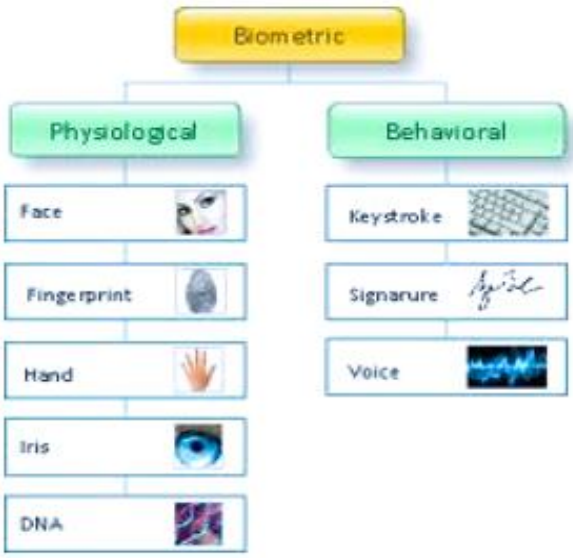

FIGURE 1: BIOMETRICS TYPES

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

3.1 Types of Biometrics

1. Facial Recognition:

Facial recognition systems work by distinguishing the face from the background. This is especially useful when identifying a person in a crowd. The system analyzes specific features of the face, such as its contours and distinctive points, which are called nodes. These nodes, about 80 in total, include features like:

- Jawline length
- Eye socket depth
- Distance between the eyes
- Cheekbone shape
- Nose width

Advantages:

1. It is not intrusive.
2. Its hands-free, and continuous.
3. It is possible to perform the scanning from a distance without the user's awareness.

Disadvantages:

1. The system may struggle to recognize faces if facial expressions change significantly.
2. If the image quality is low, the system may not have enough detail to recognize the face correctly.

FIGURE 2:Facial Recognition

2. Keystrokes

The purpose of this biometric system is to measure dwell time (the duration a key is held down) and flight time (the time taken to move from one key to another) during keyboard actions. Keystroke biometrics rely on extracting multiple features to construct a user's profile, which can then be used for identification or authentication. Keystroke analysis involves examining factors such as frequency, accuracy, pauses between keystrokes, and the duration of key presses.

Advantages:

1.Simplicity in Implementation: Keystroke recognition systems are straightforward to implement since they do not necessitate any specialized hardware.

2.Ease of Learning: The system is relatively easy for users to learn and adapt to.

Disadvantages:

1.Performance Variability: The effectiveness of keystroke biometrics can be influenced by various user conditions, such as hand injuries or fatigue.

2.Accuracy Limitations: These systems may have limitations in terms of accuracy.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

FIGURE 3: Keystrokes

IV. INTRUSION DETECTION SYSTEM

4.1 What is intrusion detection system?

An Intrusion Detection System (IDS) monitors all incoming and outgoing network activity to identify suspicious patterns that may indicate a network or system attack. Its main purpose is to alert when it detects unusual activity that could be an attempt to break into or compromise a system.

How It Works:
1. Monitoring Network Activity: IDS constantly checks the performance and activities of computers and networks.
2. Alerting Suspicious Activity: When it finds something suspicious, it sends an alert to inform that there might be a security threat.
Example: Gmail's Basic IDS
Gmail uses a basic form of IDS. It allows users to see if anyone has signed into their account from a different location. If you only see your own IP address and phone number, everything is fine. But if you notice an IP address from another city or country, it means someone else might have accessed your account. Gmail relies on users to check this manually, but there are also automated systems that detect suspicious activity and send warnings.

Comparing IDS to a Burglar Alarm:
Think of an IDS like a burglar alarm:
Car Example: A car lock protects the car from theft. If someone breaks the lock, the burglar alarm goes off to alert the owner. Similarly, an IDS works with a firewall to protect a network. If someone breaks through the firewall, the IDS detects it and alerts the system administrator.

Why IDS is Important:
1.Firewall Limitations: Firewalls do a good job of filtering incoming traffic from the Internet but can be bypassed in some ways. For example, an intruder might connect through a modem directly to a private network, which the firewall wouldn't detect.
2. Comprehensive Monitoring: IDS monitors not only external threats but also potential attacks or misuse from within the organization.

4.2 Types of Intrusion Detection Systems

1. Network-Based Intrusion Detection: This type operates at the network gateway, monitoring all incoming packets. It utilizes network-based sensors to detect potential threats.
2. Router-Based Intrusion Detection: Installed on routers, this type prevents unauthorized access to the network by monitoring and analyzing router traffic.
3. Host-Based Intrusion Detection: This type relies on audit data from the host's operating system, analyzing generated events to ensure the security of the local node [9],[10].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

V. FINGERPRINT RECOGNITION

Fingerprint recognition is the method of creating a digital representation of a fingerprint and comparing it with a previously stored digital version. Electronic fingerprint scanners work by capturing digital images of fingerprints. This is achieved through various techniques such as analyzing light reflections from the ridges and valleys of the fingerprint, using ultrasonic waves, or assessing the electrical properties of the finger's ridges and valleys. The captured images are then transformed into digital templates that highlight the unique features of the fingerprint. These templates can be stored in databases and utilized for secure access control. Instead of entering a password, users can place their finger on an electronic scanner, which compares the live fingerprint with the stored template to verify the user's identity and access rights [10].

Fingerprint recognition is favored among biometric techniques due to several advantages:
1.Universality: A large portion of the population has clear fingerprints, often more so than the number of people who possess passports.
2.High Distinctiveness: Even identical twins, who share the same DNA, have unique fingerprints.
3.High Performance: Fingerprints are fully developed by the age of seven months in a fetus and remain unchanged throughout life unless altered by injury or skin conditions. Even minor injuries do not permanently alter fingerprints, as the pattern regenerates as the skin heals.

5.1 Fingerprint Identification Algorithm:

A fingerprint identification system has two main processes: enrollment and authentication [10].

Enrollment Process:

1.Capturing Fingerprint: A device is used to capture a person's fingerprint.
2.Saving Fingerprint: The system saves this fingerprint in a database for future reference.

Authentication Process:

1.Verifying Identity**:** When the person wants to prove their identity, their fingerprint is captured again.
2.Comparing Fingerprints**:** The system compares the new fingerprint with the one saved during enrollment.
3.Matching:

- If the fingerprints match, the system confirms the person's identity and grants access (like unlocking a computer).
- If they don't match, the system sends an alert indicating a mismatch.

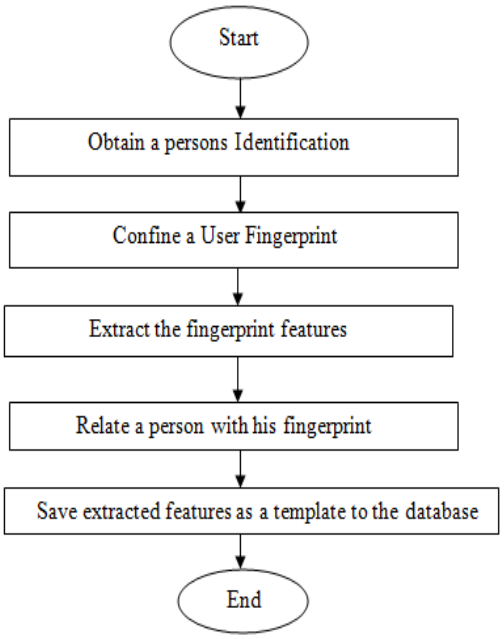

FIGURE 4. ENROLLEMNT PROCES:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

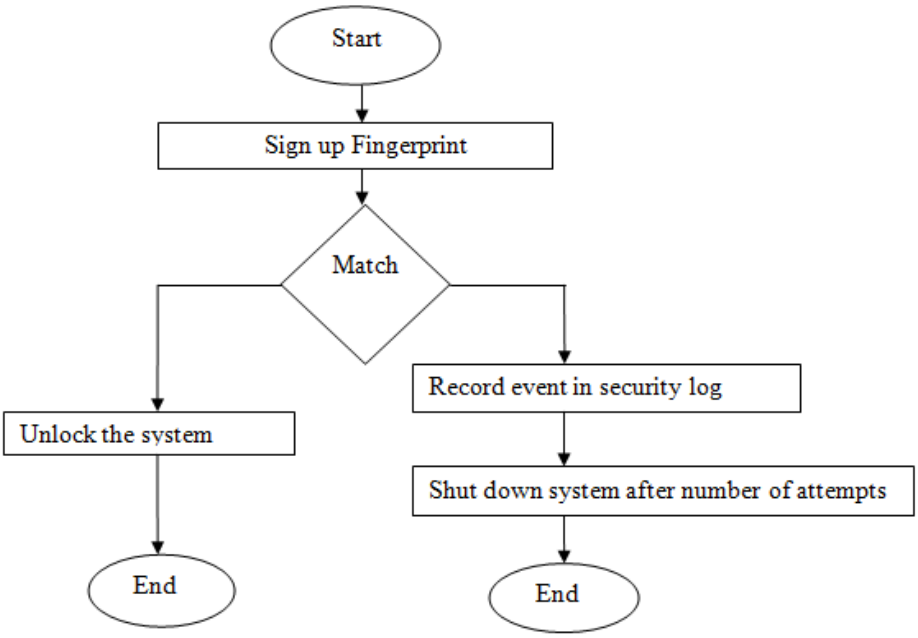

FIGURE 5. VERIFICATION PROCESS

5.2 Comparison with other techniques

1. Some people don't use a mouse often in their work, so a system that verifies identity based on mouse usage won't work for them. However, everyone can use a fingerprint-based system because everyone has fingerprints and can enroll them easily. This makes fingerprint systems more universally applicable for authentication.

2. An attacker might be able to mimic someone's typing style to access sensitive information without being detected. However, a fingerprint cannot be easily copied, making it a more secure method for verifying someone's identity.

3. The difference between fingerprint systems and mouse or keystroke systems is mainly in the time they take to work effectively:

Mouse Dynamics and Keystroke Techniques are systems need a lot of time to learn how a user moves their mouse or types. This training can take hours or even days, and it also takes longer to verify the user each time Fingerprint Identification System is much faster. It only takes a short time to enroll a fingerprint and quickly verifies the user each time.

VI. CONCLUSION

Using identification tools alongside intrusion detection systems can help reduce attacks aimed at accessing computer systems without authorization. Biometric technologies, which rely on unique biological characteristics, are considered the most reliable for this purpose. Until recently, Fingerprinting biometrics were commonly used because they don't require special devices. However, some studies have shown that these techniques are not very effective.

As a result, researchers have been motivated to develop identification systems based on fingerprint technology. Fingerprint-based systems are more efficient and accurate compared to behavioral biometrics, making them a better choice for enhancing security alongside intrusion detection systems.

REFERENCES

[1]. FaizKhademi, A., Zulkernine, M., & Weldemariam, K. (2015). Fpguard: detection and prevention of browser fingerprinting., 293-308.

[2]. PONNUSAMY, P., Monickaraj, V., & PERIYATHAMBI, E. (2022). Efficient intrusion detection and prevention model in cloud environment using sgd-lstm and c2ha. Studies in Informatics and Control, 31(2), 95-104.

[3]. Al-Fannah, N. and Mitchell, C. (2020). Too little too late: can we control browser fingerprinting?.Journal of Intellectual Capital, 21(2), 165-180.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 6, June 2024

DOI: 10.17148/IJARCCE.2024.13637

[4]. A.Ahmed and I. Traore. Anomaly intrusion detection based on biometrics. In 6th IEEE Information Assurance Workshop, 2005.

[5]. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. In Transactions on Dependable and Secure Computing, pages 165–179, 2007.

[6]. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics: a grand challenge. In Proceedings of the 17th International Conference on Pattern recoginition, pages 935–942, 2004.

[7]. D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM transactions on information and System Security, 8(3), 2005.

[8]. E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics. In Computer and Network Security, Massachusetts Institute of technology, 2004.

[9]. J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.

[10]. Khalil Challita, Hikmat Farhat, Khaldoun Khaldi. Biometric Authentication for Intrusion Detection Systems In Proceedings of the First International Conference on Integrated Intelligent Computing,2010.